1

Medical Equipment Management in Healthcare Facilities

1.1. Introduction

Healthcare facilities, whether public hospitals, private clinics, or specialized centers, are at the heart of the modern care system. Their core mission is to ensure access to quality, safe and equitable care in environments where human, material and informational resources must coherently interact. In this context, medical equipment, which forms the technological backbone of care delivery, plays a strategic role. It enables healthcare professionals to diagnose accurately, treat effectively and continuously monitor patients (David and Jahnke 2004).

Healthcare facilities, from major public hospitals to private clinics, constitute the cornerstone of the modern healthcare system. Their core mission is to ensure access to high-quality, safe and equitable care within an environment where human, material and informational resources must function in a coherent and integrated manner. Medical equipment, serving as the technological backbone of care delivery, plays an essential strategic role. It supports accurate diagnosis, effective treatment and continuous patient monitoring. Moreover, the growing connectivity of these devices – often referred to as the Internet of Medical Things (IoMT) – positions them as vital nodes within the broader healthcare information ecosystem.

This increasing reliance on technology, however, introduces critical vulnerabilities. Equipment failure is no longer merely a technical

inconvenience; it represents a potential rupture in the care continuum, leading to diagnostic delays, therapeutic interruptions and compromised patient safety. Traditional maintenance models, which tend to be reactive or based on fixed schedules, have proven to be both inefficient and costly.

To address these challenges, our research proposes a sophisticated predictive maintenance methodology aimed at transforming biomedical asset management. This approach is built upon three foundational pillars. First, Weibull analysis leverages historical failure data to transition from calendar-based to condition-based maintenance (CBM) using statistical modeling to estimate failure probabilities and remaining useful life. Second, fault tree analysis (FTA) provides a deductive, hierarchical framework for identifying all potential technical, human and procedural causes of failure, enabling a deeper understanding of root causes. Finally, Bayesian networks (BN) integrate these elements into a dynamic intelligence system, continuously updating failure risks in real time, based on incoming data from sensors and performance tests.

The operational goal of this integrated methodology is to enable proactive and precisely targeted maintenance. In practice, the system will generate early warnings – such as "component Y has a 92% probability of failure within the next fifteen days" – allowing interventions to be scheduled during periods of low clinical activity, thereby minimizing disruption.

The benefits extend across the entire healthcare ecosystem. Facilities will achieve greater equipment availability, optimized maintenance budgets and more efficient allocation of technical resources. Clinicians will gain confidence and operational serenity and be able to focus on patient care without unexpected technical interruptions. Most importantly, patients – the ultimate beneficiaries – will experience enhanced safety and care continuity, contributing to better health outcomes and a more reliable care experience.

In summary, this modernization of maintenance practices transcends technical improvement – it supports the broader objective of strengthening the resilience and performance of the entire healthcare system. By making technology a dependable and efficient lever, we put it firmly at the service of human health.

1.2. The central role of medical equipment in care delivery

Medical devices are a fundamental pillar of modern medicine, covering an extremely broad spectrum of tools and technologies. This range extends from surgical instruments and radiology equipment to laboratory devices, physiological monitors and infusion pumps. Life-support equipment, such as defibrillators, incubators and ventilators, represents a crucial category for maintaining vital functions. Today, this physical dimension is complemented by a growing digital dimension, with the integration of solutions such as electronic health records and telemedicine, which are revolutionizing health data management (World Health Organization 2025). The presence of these technologies is now ubiquitous and systemic, spanning the entire patient care pathway. Their use begins in emergency departments for diagnosis and immediate stabilization, continues in intensive care units for continuous monitoring and life support, and extends into rehabilitation departments, where they play a key role in recovery and long-term follow-up.

Technological advances have profoundly transformed the hospital ecosystem, notably bringing about a revolution in task automation, diagnostic accuracy and rapid intervention. However, this growing sophistication, while synonymous with progress, introduces operational complexity that requires rigorous management and dedicated expertise. Indeed, medical devices, although designed to save lives, can paradoxically become the source of critical clinical failures. The slightest technical failure, a human–machine interface error, or a targeted cyberattack can compromise patient safety, delay urgent care or, in the worst case, lead to medical errors with dramatic consequences (Arya et al. 2019).

Beyond purely technical risks, this increased dependence on technology raises major human and organizational challenges. It requires ongoing training for caregivers to ensure perfect mastery of the tools, demanding preventive maintenance, and seamless interoperability between systems to guarantee continuity and traceability of care. Thus, the modern hospital must find a delicate balance: fully leveraging the innovative potential of technology while mitigating the risks it generates, so that progress always translates into enhanced patient safety.

The proper functioning of these devices depends on multiple factors: maintenance, component quality, compatibility with hospital software and regular firmware updates. Moreover, increased reliance on digital equipment

introduces new vulnerabilities, particularly cybersecurity risks, which must be integrated into the hospital's overall risk management strategy (Tully et al. 2020).

The reliable and secure operation of these devices depends on a multitude of interdependent factors, forming a complex technical and organizational ecosystem. Critical elements include stringent preventive and corrective maintenance protocols, high intrinsic quality and full traceability of components, seamless integration and compatibility within hospital software architectures, and the consistent and timely application of software and firmware updates – essential for addressing vulnerabilities and sustaining performance.

Moreover, growing dependence on interconnected digital equipment introduces emerging risks, notably in the domain of cybersecurity. Threats such as ransomware, data breaches and attacks on critical systems cannot be addressed in isolation. Proactive and continuous management of these risks must be comprehensively and cross-functionally embedded into the healthcare facility's overall risk management strategy. Such integration is vital in ensuring the resilience of the hospital information system, safeguarding patient data confidentiality and ultimately upholding the continuity and safety of care in an increasingly digital environment (Tully et al. 2020).

1.3. Organization and responsibilities of the biomedical maintenance department

The integrity of medical equipment, which is fundamental to patient safety and the uninterrupted delivery of care, is entrusted to a highly specialized unit known as the Biomedical Engineering Department. More than just a technical support team, this department functions as a multidisciplinary hub where biomedical engineers and technicians integrate expertise across electronics, information technology, precision engineering and healthcare regulations. Its responsibilities extend well beyond remedial repairs to include holistic management of the medical device inventory. This encompasses technical activities – such as performing device calibrations, software upgrades and hardware interventions – as well as organizational functions like systematic scheduling of preventive maintenance and maximizing the operational readiness of critical care equipment. In addition, the department maintains comprehensive documentation, including service

records, compliance certificates and full traceability of components. This ensures not only reliable equipment performance but also adherence to stringent regulatory standards and the capacity to review all actions for future audits or incident analyses. Through its integrated approach to technical, operational and documentary oversight, the biomedical engineering department serves as an indispensable component in the resilience and efficiency of the healthcare system.

Medical equipment maintenance is handled by a specialized unit: the biomedical maintenance department. This department manages the technical, organizational and documentation aspects of the biomedical inventory. Its key responsibilities include the following:

– *Inventory management*

The implementation of an intelligent, centralized and relational database enables comprehensive traceability and advanced strategic analysis of medical equipment. This sophisticated system integrates key parameters such as device category and classification, precise physical location (department, unit, floor, building), detailed manufacturer information including technical support contacts and service level agreements, acquisition dates, commissioning timelines, warranty status with expiration tracking and a complete historical record of all interventions – including preventive maintenance, corrective actions, calibration certificates, software updates and user-reported observations. This structured framework not only streamlines maintenance scheduling and optimizes equipment availability but also provides actionable, data-driven insights to support strategic decisions related to lifecycle management, fleet standardization, resource allocation and procurement planning. Advanced analytics capabilities further enhance operational efficiency by identifying usage patterns, predicting maintenance needs, and minimizing downtime through proactive intervention.

– *Preventive maintenance*

Planned in strict accordance with manufacturers' specifications and current technical standards, preventive maintenance serves as a foundational element of effective biomedical equipment management. It extends beyond routine scheduled tasks by incorporating data-driven insights from failure history analytics, usage patterns and operational context. Through systematic

performance verification, comprehensive cleaning protocols, precision calibration and proactive replacement of high-risk components, this approach substantially decreases unexpected equipment failures and enhances device longevity. By maintaining devices in optimal operating condition, it improves clinical workflow efficiency, ensures consistent performance accuracy and, most importantly, safeguards patient safety by reducing the potential for equipment-related adverse events. Furthermore, it embodies a philosophy of continuous improvement: each maintenance activity contributes to an expanding knowledge repository, enabling refinement of maintenance intervals, procedures and overall asset management strategy.

– *Corrective maintenance*

Initiated in response to equipment failure or user reports, corrective maintenance responses are prioritized based on the clinical criticality and operational impact of each incident. For failures that compromise patient safety or disrupt urgent clinical procedures, immediate intervention is mandatory. For non-critical equipment or minor malfunctions, deferred maintenance may be scheduled to optimize resource allocation without affecting patient care. Successful execution depends on responsive logistical support – including strategic inventory management of spare parts, access to specialized diagnostic equipment and the availability of qualified technical staff – coupled with comprehensive documentation that cover fault diagnosis, repair actions, components replaced and equipment downtime. This systematic approach not only restores equipment function but also supports continuous improvement through root cause analysis and ensures adherence to regulatory standards and accreditation requirements (Leming et al. 2023).

– *Quality control*

Beyond routine maintenance, critical medical devices demand a rigorous regime of periodic performance verification, compliance audits and precise calibration or recalibration to guarantee both metrological integrity and clinical validity. These systematic quality assurance processes – mandated by strict international standards (such as ISO 9001, ISO 13485 and IEC 62353) and regulatory guidelines – ensure that all measured parameters (e.g. pressure, flow, radiation dosage, electrical current and temperature) remain accurate, traceable and consistent across the entire device lifecycle. Each operation is documented in detail, creating an auditable trail that captures

measurement results, adjustments made and compliance status. This end-to-end traceability not only safeguards patient safety by preventing diagnostic errors and therapeutic inaccuracies but also supports institutional accreditation, reinforces legal compliance and fosters a culture of excellence in clinical engineering.

– *User training and competency assurance*

Inadequate operator technique remains a significant source of premature device degradation, preventable operational faults and adverse clinical events. To mitigate these risks, structured training programs – delivered through competency-based learning pathways including hands-on sessions, simulation-based exercises and digital learning platforms – are systematically developed and integrated into the clinical technology management lifecycle. These educational interventions address essential operational protocols (power-up, routine operation and safe shutdown), as well as advanced topics such as cleaning and disinfection procedures, early error recognition, anomaly reporting workflows and emergency response actions. Sustained and role-specific training implementation directly enhances device reliability, reduces use-related hazards, extends asset service life and strengthens clinical staff proficiency and autonomy (Kremer et al. 2023).

Implementation of an integrated Computerized Maintenance Management System (CMMS) serves as a foundational enabler for data-informed maintenance orchestration and end-to-end process traceability. These enterprise platforms provide centralized oversight and automation of the entire medical equipment support ecosystem, including real-time asset status monitoring, intelligent scheduling of preventive maintenance and calibration activities, spare parts inventory management and root-cause analysis of failure trends.

Furthermore, advanced CMMS solutions generate key performance indicators – for example, mean time between failures (MTBF), overall equipment effectiveness (OEE), maintenance cost-per-use and compliance rate – enabling evidence-based decision-making, predictive maintenance modeling, strategic resource planning and continuous enhancement of clinical engineering services in alignment with patient safety and organizational performance goals.

1.4. Regulatory and normative framework of medical devices

The medical device sector encompasses a rapidly evolving technological landscape, extending from fundamental surgical instruments to advanced artificial intelligence (AI)-based diagnostic software and connected health solutions. This dynamic field is governed by a sophisticated regulatory framework designed to balance two critical objectives: ensuring patient safety and product efficacy while simultaneously promoting innovation and timely market access. These regulations form a multi-tiered structure operating at international, regional and national levels, creating both challenges and opportunities for manufacturers and healthcare providers.

The regulatory ecosystem rests upon two fundamental pillars:

– *Regulations*

Regulations such as the European Union's Medical Device Regulation (MDR) 2017/745 and the U.S. Food and Drug Administration's (FDA) Quality System Regulation (21 CFR Part 820) establish mandatory legal requirements that devices must satisfy before and after market entry. These binding instruments govern critical aspects including product classification, conformity assessment procedures, unique device identification (UDI) systems, clinical evidence requirements, post-market surveillance and incident reporting protocols. They carry the force of law and are enforced by regulatory authorities through audits, inspections and market surveillance activities.

– *Technical standards*

Technical standards, including ISO 13485 (Quality Management Systems), IEC 60601 (Safety and Essential Performance) and ISO 14971 (Risk Management) – while typically voluntary in application – provide the necessary technical detail and methodologies to demonstrate compliance with regulatory requirements. These consensus-based documents, developed by international standardization bodies, offer precise engineering specifications, validation methodologies and best practices covering design, manufacturing, testing, risk management and documentation. Their application provides manufacturers with predictable pathways to conformity and facilitates global market access through harmonized technical requirements.

Together, regulations and standards create a coherent framework that ensures medical devices throughout their entire lifecycle, from initial concept and design through production, clinical use and eventual decommissioning, and meet consistently high standards of safety, performance and quality. This document provides a comprehensive overview of the international and European regulatory landscape, detailing the essential technical standards that govern medical devices and examining the ongoing challenges in global regulatory harmonization. It further explores how emerging technologies, such as AI-driven diagnostics, wearable medical devices and digital health applications, are reshaping regulatory paradigms and creating new requirements for evidence generation, cybersecurity and lifecycle management.

1.4.1. *Typology of regulations applicable to medical devices*

1.4.1.1. *Regulatory frameworks by geographic area*

Medical devices are subject to specific legal requirements, depending on the markets where they are commercialized. These regulatory frameworks establish the conditions for access to each market and define the legal obligations of manufacturers.

1) *Supranational regulations*

Regulation (EU) 2017/745 on medical devices (MDR) constitutes the binding legal framework for all member states of the European Union. It introduces a reinforced approach to clinical evaluation, imposes an extensive product traceability system through UDI and establishes strict post-market surveillance requirements. Its application is mandatory for any marketing within the European Economic Area.

2) *National regulations*

Each country has its own regulatory system. In the United States, the Food and Drug Administration (FDA) enforces Title 21 CFR Part 820 (Quality System Regulation), which governs manufacturing practices, as well as distinct approval processes such as Premarket Notification 510(k) for substantially equivalent devices or Premarket Approval (PMA) for innovative technologies. Japan follows the Pharmaceutical and Medical

Device Act under the supervision of the PMDA, while China enforces NMPA regulations with specific requirements for local clinical trials.

1.4.1.2. *Cross-cutting technical and process requirements*

Beyond geographical boundaries, certain technical requirements apply universally and concern all manufacturers, regardless of their location.

1) *Quality and risk management requirements*

The implementation of a system of quality management compliant with ISO 13485 has become a nearly mandatory requirement for operating in international markets. Although technically a standard, its adoption is required by regulatory authorities as proof of compliance with quality and safety principles. Similarly, the application of ISO 14971 for risk management is systematically required to demonstrate a structured approach to risk assessment and control.

2) *Traceability and identification requirements*

The UDI (Unique Device Identifier) system was made mandatory by the European MDR and US FDA regulations. It requires manufacturers to assign unique identifiers to each device, record this information in centralized databases and maintain complete traceability from production to the patient. This system not only enables targeted and effective recalls but also improves monitoring of real-world device performance.

3) *Vigilance and post-market surveillance requirements*

Modern regulations place particular emphasis on continuous post-market surveillance. The MDR requires the systematic transmission of incident reports via the Eudamed system and the regular production of periodic safety reports. The FDA maintains the MAUDE system to collect adverse event reports, while other markets such as Canada and Australia have implemented similar systems. These mechanisms enable rapid problem detection and ongoing benefit–risk assessment.

4) *Specialized requirements and recommendations*

In response to emerging technologies, authorities develop specific guidance documents. The FDA's guidance on cybersecurity of connected

devices or the evaluation of AI algorithms establishes detailed technical expectations. Although not legally binding, these documents reflect the regulators' stance and have become essential references for obtaining marketing authorizations.

1.4.2. *Typology of standards applicable to medical devices*

1.4.2.1. *Quality management: the foundation*

ISO 13485:2016 serves as the cornerstone of Quality Management Systems (QMS), particularly the medical device industry. Unlike ISO 9001, which emphasizes customer satisfaction, ISO 13485 prioritizes device safety, regulatory compliance and risk mitigation. It establishes a rigorous framework to ensure that all processes, including design, installation, production, development and servicing, are consistently controlled and documented. Key applications span technical documentation, supplier qualification, production oversight and management of non-conforming products. Compliance is often a legal prerequisite for obtaining CE marking (under EU MDR) or FDA approval (under 21 CFR Part 820) and is rigorously audited by notified bodies and regulatory authorities.

1.4.2.2. *Risk management: the cornerstone of safety*

ISO 14971:2019 defines a comprehensive framework for risk management throughout a medical device's lifecycle. It guides manufacturers in systematically identifying, evaluating and controlling risks associated with device use. The process encompasses hazard analysis, risk assessment, implementation of mitigation measures, evaluation of residual risks and continuous post-market surveillance. This standard is indispensable for demonstrating to regulators (e.g. under EU MDR or FDA requirements) that a device's benefits outweigh its risks. It seamlessly integrates with ISO 13485, embedding risk-based decision-making into the QMS.

1.4.2.3. *Safety of medical electrical equipment*

The IEC 60601-1 series specifies essential requirements for the electrical, mechanical and thermal safety of medical electrical equipment. Its primary goal is to protect patients and operators from hazards such as electric shock, excessive temperatures, radiation exposure and mechanical failures. Applicable to all electrically powered medical devices (e.g. ventilators, defibrillators and patient monitors), it mandates stringent testing for

insulation integrity, electromagnetic compatibility (EMC), mechanical stability and environmental resilience. Compliance is legally mandatory for market access in most global jurisdictions.

1.4.2.4. *Medical software lifecycle*

IEC 62304:2006 outlines lifecycle requirements for medical software, whether embedded within hardware or operating as standalone Software as a Medical Device (SaMD). It classifies software into three risk categories:

– *Class A*: No injury or damage possible.

– *Class B*: Non-serious injury possible.

– *Class C*: Death or serious injury possible.

Development, testing and documentation activities are scaled accordingly. With the rise of AI-driven diagnostics, telehealth platforms and mobile health apps, this standard ensures software reliability, security and traceability.

1.4.2.5. *Labeling and user information*

ISO 20417:2021 standardizes manufacturer-provided information, including labels, instructions for use (IFU) and technical documentation. It requires content to be clear, accessible and linguistically tailored to the end-user's region. By defining minimum labeling elements (e.g. device name, manufacturer details and UDI), structuring IFUs for usability and specifying safety warnings, this standard reduces use errors and aligns with the transparency mandates of regulations such as EU MDR.

1.4.2.6. *Cybersecurity management for medical devices: ISO/TS 20443*

This technical specification addresses the critical intersection of cybersecurity and patient safety in connected medical devices (ISO 13485). Unlike general information security standards, ISO/TS 20443 provides a tailored framework for the unique ecosystem of medical technology, focusing specifically on protecting the confidentiality, integrity and availability of health data while ensuring that security measures do not compromise device functionality or patient safety. It applies to both manufacturers developing connected devices (e.g. implantables, monitoring systems and SaMD) and healthcare organizations deploying these

technologies. Key requirements include robust encryption protocols, vulnerability management processes, granular access controls and comprehensive incident response planning. As medical devices become increasingly interconnected and targeted by cyber threats, this standard offers a proactive approach to mitigating risks that could directly impact clinical operations and patient outcomes. Although still emerging, it is rapidly becoming a vital reference for complying with evolving regulatory expectations – including EU MDR cybersecurity annexes and FDA premarket guidance – and for building trust in digital health solutions.

At the hospital level, these requirements translate into strict procedures for technical acceptance, periodic servicing, decommissioning and materiovigilance. Regulatory audits also demand documented evidence of maintenance, tracking of technical alerts and corrective actions planes (European Commission 2017).

1.5. Managing uncertainty and random data

Maintenance of biomedical equipment presents a complex challenge due to the inherent uncertainty characterizing technical failures. Unlike some industrial sectors where failures often follow predictable patterns, medical devices are subject to numerous variable factors that make their maintenance particularly demanding. Usage intensity varies considerably across departments: a ventilator in intensive care operates continuously under maximum demand, while the same model in a standard care unit experiences more moderate use. This disparity results in radically different wear patterns that cannot be modeled using traditional approaches.

Environmental conditions represent another critical parameter. Excessive heat in sterilization rooms, humidity in operating theaters or electromagnetic interference in medical imaging create invisible but constant stresses on electronic and mechanical components. The same equipment may demonstrate completely different reliability, depending on its installation environment, challenging conventional preventive maintenance standards.

The human dimension is perhaps the most unpredictable factor. The considerable variation in technical skills among healthcare staff, combined with time pressures in clinical settings, creates demands that are sometimes unanticipated by manufacturers. Repeated improper handling during sensor

connection, aggressive cleaning protocols or minor but frequent mechanical impacts can cause cumulative damage that standard protocols struggle to anticipate.

The advent of connected devices has introduced a new dimension of uncertainty: software interoperability. Updates to hospital information systems, conflicts between software versions or simply the complexity of interfaces between equipment from different manufacturers create systemic vulnerabilities. A failure may therefore stem not from a hardware defect, but from software incompatibility that emerges months after installation.

Faced with this complexity, biomedical maintenance departments must implement sophisticated strategies combining continuous IoT monitoring, predictive analytics using AI and adaptive user training programs. Maintenance is evolving from scheduled-based approaches to dynamic risk analysis methodologies, where the clinical criticality of each device determines the required supervision levels. Real-time data from embedded sensors enable detection of subtle anomalies long before they develop into full failures.

This transformation requires close collaboration between biomedical engineers, clinicians and information technology specialists. User feedback has become an essential source of intelligence for continuously improving prediction models. The objective is no longer to eliminate uncertainty – an impossible mission – but to develop organizational resilience to address it effectively, ensuring patient safety remains the absolute priority regardless of technological complexity.

1.5.1. *Sources of uncertainty in biomedical equipment maintenance*

Uncertainty in biomedical equipment maintenance arises from multiple interconnected factors that complicate prediction and planning efforts, creating a complex ecosystem of variables that challenge even the most sophisticated maintenance protocols.

– *Variability in failure patterns*

Identical device models may demonstrate significantly different failure characteristics and lifespans due to microscopic manufacturing variations,

component sourcing differences and subtle production modifications over time. This stochastic behavior presents substantial challenges for accurate failure prediction, as traditional reliability models based on MTBF often prove inadequate for capturing the full spectrum of potential failure scenarios in medical devices.

– *Insufficient historical data*

Newly acquired devices, rarely used specialized equipment, or recently modified systems often lack comprehensive maintenance histories. This data scarcity impedes reliable statistical analysis and hinders the development of evidence-based maintenance strategies, particularly for predicting rare but critical failure modes that may only emerge after extended periods of operation or under specific clinical conditions.

– *Deviation from intended use conditions*

Clinical environments frequently deploy equipment in ways not anticipated by manufacturers, creating unexpected operational contexts that accelerate degradation. Devices may operate beyond recommended duty cycles, manage patient loads exceeding specifications or function in clinical scenarios not envisioned during the design phase, thereby accelerating wear and generating novel failure modes that bypass conventional diagnostic protocols.

– *Complex human–device interactions*

Many failures originate from use errors, inadequate training or workflow adaptations that introduce unanticipated stresses on equipment. These include improper calibration procedures, incorrect cleaning techniques, undocumented workarounds and accidental damage during emergency situations. Variability in operator skill levels and clinical experience further compounds these challenges, creating a layer of operational uncertainty that is difficult to quantify and mitigate through technical measures alone.

– *Environmental and cybersecurity threats*

Equipment performance is influenced by environmental conditions including temperature fluctuations, humidity levels, airborne contaminants and electromagnetic interference, which can degrade components and affect measurement accuracy. Furthermore, connected medical devices face

growing vulnerabilities to malware infections, ransomware attacks and unauthorized access attempts that can compromise functionality and data integrity, introducing digital risk factors that traditional maintenance approaches are ill-equipped to address (Stawowy et al. 2021).

1.5.2. *Extended implications*

These uncertainty sources generate cascading effects on clinical operations that extend beyond immediate technical concerns. Unplanned downtime can disrupt patient care pathways, necessitate procedure rescheduling and increase dependence on backup equipment, potentially affecting clinical outcomes and patient safety. Financially, uncertainty leads to either excessive preventive maintenance (increasing operational costs and potentially causing unnecessary wear from frequent interventions) or insufficient maintenance (heightening failure risks and potentially leading to more severe consequences). Strategically, this environment demands adaptive maintenance approaches that balance resource allocation with clinical priorities while maintaining regulatory compliance across diverse equipment portfolios, requiring sophisticated risk assessment frameworks that can account for both technical and operational variables in healthcare settings.

1.6. Probabilistic methods

Probabilistic methods provide a mathematical framework to quantify uncertainties in biomedical equipment failures through statistical analysis of historical data. These approaches transform complex failure phenomena into predictive tools that optimize maintenance strategies, improve resource allocation and enable anticipation of critical failures. Their application spans all device categories, from basic electronic thermometers to advanced medical imaging systems, although their effectiveness varies significantly across different failure modes and device types.

1.6.1. *Weibull distribution*

The Weibull distribution models variable failure rates through its shape parameter β (indicating increasing, constant or decreasing failure rates)

and scale parameter η (representing characteristic lifetime) (Chowdhuri et al. 2023). Particularly effective for mechanical and electromechanical components subject to wear mechanisms, it enables prediction of residual life and planning of targeted preventive maintenance. However, its application requires substantial failure data (typically exceeding 30 data points) for reliable parameter estimation and demonstrates limited effectiveness for failures originating from cyberattacks, human errors or software-related issues. The distribution's flexibility makes it valuable for modeling aging processes in infusion pumps, mechanical ventilators and surgical instruments.

1.6.2. *Exponential distribution*

As a particular case of the Weibull distribution (where $\beta = 1$), this model assumes constant failure rates over time. Mathematically straightforward to implement, it primarily suits electronic components and software systems where failures occur randomly and independent of time. While useful for preliminary modeling, its assumption of constant failure rate renders it inappropriate for devices exhibiting progressive wear patterns, and it may significantly underestimate risks when applied to equipment with time-dependent degradation mechanisms. The distribution finds appropriate application in solid-state electronics and embedded systems where failure mechanisms are truly random.

1.6.3. *Log-normal distribution*

This distribution models progressive degradation processes where the logarithm of failure times follows a normal distribution. It effectively represents cumulative wear in electrochemical components such as defibrillator batteries, physiological sensors and imaging system detectors.

The model provides realistic representations of gradual degradation but presents challenges in parameter interpretation and demonstrates sensitivity to preventive maintenance interventions. Its mathematical properties make it particularly suitable for modeling failure mechanisms dominated by diffusion processes or chemical degradation.

1.6.4. *Other distributions*

The gamma distribution generalizes the exponential distribution to model time until the *k*th failure in redundant systems, making it valuable for analyzing backup power systems and fault-tolerant architectures. The homogeneous Poisson process models failure counts over specified intervals with constant occurrence rates, proving useful for high-frequency failure events in patient monitoring equipment and mobile medical devices. More complex models, including Gaussian mixture distributions, address multifunctional devices with heterogeneous failure modes, although they require sophisticated parameter estimation techniques.

1.6.5. *AI integration and real-time data*

Contemporary approaches integrate traditional probabilistic methods with AI through several advanced methodologies. Machine learning algorithms, particularly survival analysis models and recurrent neural networks, incorporate multi-source operational data including usage patterns, environmental conditions and error logs to enhance prediction accuracy. Digital twin technology creates virtual replicas that simulate failure scenarios under varying operational conditions, enabling optimization of maintenance strategies through computational modeling. These advanced methods significantly improve failure prediction for complex systems but require substantial computational resources and specialized expertise for implementation.

1.6.6. *Limitations and future directions*

The effectiveness of probabilistic methods remains constrained by several fundamental factors. Data quality issues, including incomplete records, reporting inconsistencies and censored data, limit model accuracy. The dynamic nature of healthcare environments, including equipment repurposing and protocol changes, challenges the stability of model assumptions. Human factors and cyber-related failures escape conventional probabilistic modeling frameworks. Future research priorities include developing explainable AI systems for clinical engineering, establishing standardized reliability data exchange protocols between institutions and

creating hybrid approaches that combine data-driven methodologies with physics-based models. These advancements aim to address current limitations while enhancing predictive capabilities for increasingly complex medical devices and systems.

1.7. Advanced predictive maintenance strategies for medical devices

1.7.1. *Analysis of reliability, maintainability and availability*

Statistical distributions are employed in the study of three key indicators to assess the performance of biomedical equipment.

– *Reliability*

Quantified by MTBF, reliability models the probability of fault-free operation of equipment over a specific period. The Weibull distribution, with its shape and scale parameters, is particularly useful for representing different failure patterns (infant mortality, useful life and progressive wear), thereby providing an essential predictive approach for strategic maintenance planning.

– *Maintainability*

Evaluated through MTTR (mean time to repair), maintainability integrates technical, logistical and human aspects of repair processes. It examines the effectiveness of corrective interventions, including spare parts availability, technical staff qualifications and post-repair validation procedures. Distributions such as log-normal effectively model the variability of intervention times, although this approach may underestimate the multifactorial complexity of failures in real clinical environments.

– *Availability*

These two dimensions are combined to calculate the effective operational rate (Availability = MTBF/(MTBF + MTTR) × 100%). This crucial indicator for care continuity provides an aggregated view that does not fully capture operational complexity, including administrative wait times, supply delays or organizational constraints.

1.7.2. *Advanced statistical tools*

– Fault trees

Deductively identify combinations of events leading to critical failures, proving indispensable for analyzing complex systems such as operating theaters or intensive care units. Their rigorous construction requires specialized expertise and a thorough understanding of system interactions.

Fault trees represent a systematic analysis method that deductively identifies combinations of events capable of causing critical failures. This approach proves particularly valuable when studying complex medical systems such as operating rooms or intensive care units, where equipment failure may lead to serious consequences.

The construction process follows top-down logic, beginning with a major adverse event and tracing backward to all potential causes through Boolean logic operators. The AND gate needs the simultaneous occurrence of all input events, while the OR gate indicates that a single input event suffices to trigger the output event.

In biomedical applications, this methodology enables analysis of critical scenarios such as intraoperative ventilation failure, while simultaneously considering hardware malfunctions, software errors, human factors and organizational deficiencies.

Rigorous implementation of this technique demands specialized expertise and profound understanding of system interactions. It additionally requires validation of assumptions by clinical experts and regular updates reflecting technological advancements.

Notable advantages include clear visualization of critical failure pathways and identification of single points of vulnerability. However, complexity escalates with system sophistication, and the method faces difficulties in fully capturing intricate human–system interactions.

Modern approaches now integrate fault trees with Monte Carlo simulations for probabilistic analysis and Bayesian networks for dynamic updating. Specialized software enables partial process automation, although human expertise remains essential for correct interpretation of results and validation of underlying assumptions.

– *Markov chains*

Model transitions between operational states (normal operation, partial failure, corrective maintenance and preventive maintenance) in dynamic systems, enabling the simulation of different maintenance strategies' impact on overall availability. Their application faces limitations in representing highly complex systems where interactions are nonlinear and multi-scale.

Markov chains provide a powerful mathematical framework for modeling transitions between distinct operational states – such as normal operation, partial failure, corrective maintenance and preventive maintenance – within dynamic systems. By representing these states and the probabilities of transitioning between them, Markov chains enable the simulation and analysis of how different maintenance strategies influence overall system availability, performance and longevity. This is especially valuable in environments like healthcare, where equipment reliability directly impacts patient outcomes. For instance, by modeling a ventilator's lifecycle – including periods of stable function, degradation, maintenance interventions and recovery – hospital engineers can quantitatively compare proactive versus reactive maintenance policies and optimize resource allocation.

However, the application of Markov chains faces significant limitations when dealing with highly complex systems characterized by nonlinear interactions and multi-scale dependencies. In real-world biomedical settings, equipment failure and repair processes often involve interdependencies that cannot be easily captured using Markovian assumptions, such as the requirement for memoryless transitions or fixed transition probabilities. For example, the failure rate of an MRI machine might depend not only on its usage patterns but also on environmental factors, software updates and human operational errors, which collectively introduce variability that challenges traditional Markov models. Additionally, systems with large numbers of states or continuous-state spaces may become computationally intractable when modeled using discrete-state Markov chains.

To address these shortcomings, modern approaches often integrate Markov chains with hybrid models or multi-scale modeling techniques. For instance, combining Markov decision processes (MDPs) with simulation-based methods allows for more flexible representation of

complex systems, while still leveraging the interpretability and analytical power of Markov chains. Advances in computational tools have also facilitated the use of hierarchical and multi-level Markov models, which can partially accommodate nonlinearities by decomposing the system into simpler, interacting subsystems. Nevertheless, human expertise remains essential to properly structure these models, calibrate them with real-world data and interpret their outcomes in context-specific scenarios – ensuring that predictions align with practical constraints and operational realities.

– *Bayesian networks*

Bayesian networks integrate structured expert knowledge and historical data to dynamically update failure probabilities in real time. Particularly suited to uncertainty management and continuous learning, their implementation requires significant statistical expertise and often encounters cultural and technical barriers in healthcare environments.

Bayesian networks represent an advanced probabilistic methodology that dynamically integrates structured expert knowledge and historical data to update failure probabilities in real time. Unlike traditional statistical approaches, these networks enable graphical modeling of cause-and-effect relationships between technical, operational and human variables, providing a systemic view of risks. Their architecture relies on probabilistic theorems that quantify the impact of new observations on initial probabilities, creating a continuous learning system particularly suited to managing uncertainties in complex environments.

In the biomedical field, this approach proves crucial for predictive monitoring of critical equipment such as intensive care ventilators or medical imaging devices. By continuously assimilating maintenance data, technical alerts and usage feedback, Bayesian networks gradually refine their predictions and identify emerging failure patterns that conventional methods might overlook. For example, they can detect that specific combinations of high humidity levels and intensive usage cycles significantly increase failure risk in certain cardiac monitor models.

However, effective implementation of these networks faces several substantial challenges. The requirement for advanced statistical expertise to design and validate network structure often presents a major obstacle,

particularly in hospital environments where specialized resources are limited. Furthermore, integrating data from heterogeneous sources (preventive maintenance records, clinical incident reports and technical parameters) requires complex preliminary standardization and robust data governance. Culturally, adoption of these tools can be hindered by reluctance to replace traditional methods with probabilistic approaches perceived as less transparent.

Despite these challenges, the advent of medical Industrial Internet of Things (IIoT) and improved software platforms are gradually facilitating deployment of these solutions. Modern Bayesian networks now incorporate machine learning capabilities that partially automate discovery of variable relationships, reducing initial dependence on comprehensive expert knowledge. Their strategic value lies in their ability to provide contextualized early warnings and support maintenance decisions based on multivariate and evolving risk understanding, ultimately contributing to enhanced patient safety and improved operational efficiency of biomedical services.

The integration of Bayesian networks with existing hospital information systems enables continuous adaptation to new clinical environments and technical constraints, representing a significant advancement in predictive maintenance strategies for medical technology management.

1.7.3. *Operational applications*

The results of these quantitative analyses guide crucial management decisions: scheduled replacement of equipment at end of economic life, optimized planning of preventive revisions based on actual device condition and strategic evaluation of cost–benefit ratios for technological upgrades.

1.7.4. *Real-time data integration*

The advent of the biomedical IIoT enables dynamic calculation of MTBF/MTTR indicators via connected sensors, early detection of reliability deviations through continuous operational data analysis and real-time adaptation of statistical models to actual usage conditions. This technological evolution nevertheless presents substantial challenges in massive data processing and cybersecurity of connected medical devices.

1.7.5. *Limitations and best practices*

Several limitations persist: maintenance data heterogeneity frequently biases historical analyses, the dual expertise required in advanced statistics and biomedical engineering remains scarce in the job market and necessary contextualization of models to clinical specificities is often underestimated in practical implementations.

1.7.6. *Perspectives*

The future of these predictive analyses lies in the synergistic integration of AI (advanced machine learning) and digital twins. These emerging technologies enable more accurate forecasting and genuinely predictive, personalized maintenance, provided that interoperable data standards are developed and biomedical maintenance teams' skills are significantly enhanced. The progressive maturation of evidence-based maintenance approaches should enable refined resource optimization while ensuring patient safety and sustainability of technological investments.

1.8. Integrating digitalization and AI into hospital maintenance

The emergence of digital technologies is fundamentally transforming medical equipment management by enabling a proactive, data-driven approach. Through the Internet of Things (IoT), medical devices are becoming smart and connected, continuously transmitting operational data such as operating parameters, critical temperatures, load cycles, abnormal vibrations and system errors. These data streams feed CBM models, where interventions are triggered only in response to measurable anomalies, thereby eliminating unnecessary maintenance while preventing unexpected failures.

More sophisticated predictive maintenance (PdM) utilizes AI to anticipate potential failures before they occur (Alkhatib et al. 2025) by analyzing complex patterns and hidden correlations within both historical and real-time data.

Advanced algorithms process these multi-source data, cross-reference maintenance histories, detect subtle deviations and estimate failure

probabilities with increasing accuracy. These systems employ machine learning for trend analysis, deep learning for recognizing complex patterns in high-dimensional data and neural networks to model nonlinear relationships between input variables and failure risks.

1.8.1. *Benefits and implications*

– *Reduction of unplanned downtime*

Anticipating critical failures enables scheduling of interventions during planned maintenance windows, avoiding disruptions during urgent clinical procedures.

– *Optimization of maintenance schedules*

Collected data allow for prioritizing interventions based on the actual condition of equipment and dynamically adjusting the allocation of technical and human resources.

– *Extended equipment lifespan*

Targeted maintenance reduces unnecessary stress and excessive preventive disassembly, preserving the mechanical and functional integrity of devices.

– *Enhanced patient safety*

Reducing unexpected failures during critical medical procedures (e.g. surgery and intensive care) directly mitigates risks to patients.

1.8.2. *Challenges and considerations*

– *Data quality and interoperability*

Prediction reliability depends on the completeness, accuracy and standardization of data from multiple sources (sensors, digital multimeters and computerized maintenance management systems).

– *Specialized skills*

Designing, deploying and maintaining these systems requires cross-disciplinary expertise in biomedical engineering, data science and computer science.

– *Cybersecurity*

Increasing connectivity of medical devices expands the potential attack surface, necessitating robust security protocols to protect both data and critical equipment functions.

– *Cultural change*

Transitioning from calendar-based to data-driven maintenance involves transforming established processes and securing buy-in from technical and clinical teams.

As these technologies mature, they are redefining the paradigms of technical and clinical management of biomedical equipment, paving the way for truly predictive maintenance integrated into the continuum of care.

1.9. Economic, environmental and strategic challenges in medical equipment management

Effective medical equipment management needs a comprehensive economic approach that extends far beyond initial acquisition costs. The global cost of ownership (TCO) encompasses numerous factors including logistics and installation, consumables and reagents, preventive and corrective maintenance, technical training and certification, software updates and cybersecurity, sterilization and disinfection procedures, and eventual end-of-life disposal or recycling.

This holistic financial perspective reveals that operational expenses typically exceed purchase prices by three to five times over a device's lifecycle.

Contemporary management trends increasingly emphasize sustainable and socially responsible practices through several innovative strategies:

– *Equipment refurbishment*

Advanced technical processes restore used medical devices to original equipment manufacturer (OEM) specifications, typically at 40%–60% of the cost of new equipment while maintaining equivalent performance and safety standards.

– *Inter-hospital resource sharing*

Strategic pooling of high-value specialized equipment through regional networks or consortium agreements maximizes utilization rates while distributing operational costs across multiple institutions.

– *Circular economy implementation*

Comprehensive recycling programs recover valuable materials (precious metals, rare earth elements and plastics) from decommissioned equipment, while proper hazardous material handling ensures environmental compliance.

– *Eco-design integration*

Preferred supplier selection based on environmental criteria including energy efficiency, reduced material footprint, design for disassembly and minimized use of hazardous substances throughout the product lifecycle (Mengual et al. 2014).

From a strategic perspective, effective biomedical fleet management directly contributes to enhanced care quality through improved equipment availability and reliability, increased patient satisfaction through uninterrupted service delivery, ensured regulatory compliance with evolving environmental and safety standards, and strengthened institutional reputation as a healthcare sustainability leader.

In an increasingly competitive healthcare landscape, the ability to maintain a technologically advanced, environmentally responsible and financially sustainable equipment ecosystem has emerged as a significant competitive differentiator. Institutions that successfully implement integrated lifecycle management strategies not only reduce operational costs but also demonstrate organizational excellence and commitment to both patient care

and environmental stewardship, ultimately positioning themselves as preferred providers in value-based healthcare systems.

1.10. Conclusion

Medical equipment has become a cornerstone of modern healthcare facilities, with its performance directly determining clinical efficiency, patient safety and organizational sustainability. Confronted with complex technical, regulatory, economic and human challenges, an integrated approach has become essential. This approach combines advanced technological tools such as AI and IoT, rigorous lifecycle equipment management, an organizational culture focused on safety and continuous anticipation of emerging risks. Biomedical maintenance can no longer be perceived as merely a support function – it represents a central strategic element for the success of 21st-century healthcare institutions, requiring a cross-functional vision that integrates digital transformation, environmental responsibility and resource optimization while ensuring excellence in care. Its evolution toward predictive, data-driven maintenance makes it an essential lever for reconciling technological innovation, economic constraints and health safety imperatives, thereby positioning biomedical services as key players in overall healthcare system performance within value-based healthcare models.